

Claims

- [c1] In a relationship between a fraud protection provider and a customer, a system for combating online fraud, the system comprising:
- a monitoring center for monitoring a suspicious email activity, the monitoring center comprising:
 - a first computer, the first computer comprising instructions executable by the first computer to allow an analysis of an investigation of a uniform resource locator;
 - a first telecommunication link configured to provide communication between a technician and the customer, such that the technician can notify the customer of a result of the investigation of a uniform resource locator and the customer can provide instructions for responding to a fraudulent attempt to collect personal information; and
 - a second telecommunication link configured to provide data communication between the monitoring center and at least one additional computer; and
 - a second computer in communication with the monitoring center via the second telecommunication link, the second computer including instructions executable by

the second computer to:

gather an incoming email message, the incoming email message comprising a uniform resource locator;

analyze the incoming email message;

based on an analysis of the incoming email message, categorize the incoming email message as a possibly fraudulent email message; and

investigate the uniform resource locator included in the incoming email message to determine whether a location referenced by the incoming email message is associated with a fraudulent attempt to collect personal information.

[c2] A system for combating online fraud as recited in claim 1, wherein the first computer comprises further instructions executable by the first computer to analyze an investigation of a uniform resource locator.

[c3] A system for combating online fraud as recited in claim 1, wherein the first computer comprises further instructions executable by the first computer to allow a technician to analyze an investigation of a uniform resource locator.

[c4] In a relationship between a fraud protection provider and a customer, a computer system for combating online

fraud, the computer system comprising:
a processor; and
a computer readable medium in communication with the processor, the computer readable medium comprising instructions executable by the processor to:

- gather an incoming email message, the incoming email message comprising a uniform resource locator;
- analyze the incoming email message;
- based on an analysis of the incoming email message, categorize the incoming email message as a possibly fraudulent email message;
- investigate the uniform resource locator included in the incoming email message to determine whether a location referenced by the incoming email message is associated with a fraudulent attempt to collect personal information; and
- initiate a response to the fraudulent attempt to collect personal information.

[c5] A computer system for analyzing a suspicious email message, the computer system comprising:
a processor; and
a computer readable medium in communication with the processor, the computer readable medium comprising instructions executable by the processor to:

parse the suspicious email message to identify a header portion of the suspicious email message, a body portion of the suspicious email message, and a uniform resource locator portion of the suspicious email message;
analyze the header portion of the suspicious email message;
analyze the body portion of the suspicious email message;
analyze the uniform resource locator portion of the suspicious email message; and
categorize the suspicious email message as a possibly fraudulent email message.

[c6] A computer system for analyzing a suspicious email message as recited in claim 5, wherein the instructions are further executable by the processor to:
based on the analysis of the header portion of the email message, assign a score to the header portion of the suspicious email message;
compare the score assigned to the header portion of the suspicious email message with a threshold score for the header portion of the suspicious email message;
based on the analysis of the body portion of the suspicious email message, assign a score to the body portion of the suspicious email message;

compare the score assigned to the body portion of the suspicious email message with a threshold score for the body portion of the suspicious email message; and based on the analysis of the uniform resource locator portion of the suspicious email message, assign a score to the uniform resource locator portion of the suspicious email message.

[c7] A computer system for analyzing a suspicious email message as recited in claim 6, wherein the computer readable medium comprises further instructions executable by the processor to:

compare the score assigned to the uniform resource locator portion of the suspicious email message with a threshold score for the uniform resource locator portion of the suspicious email message; and

based on the comparison of the score assigned to the uniform resource locator portion of the suspicious email message and the threshold score for the uniform resource locator portion of the suspicious email message, categorize the suspicious email message as a possibly fraudulent email message.

[c8] A computer system for analyzing a suspicious email message as recited in claim 6, wherein the computer readable medium comprises further instructions executable by the processor to:

compute a composite score based on the score assigned to the header portion of the suspicious email message, the score assigned to the body portion of the suspicious email message and the score assigned to the uniform resource locator portion of the suspicious email message; assign the composite score to the suspicious email message;

compare the composite score assigned to the suspicious email message with a threshold composite score for the suspicious email message; and

based on the comparison of the composite score assigned to the suspicious email message and the threshold score for the suspicious email message, categorize the suspicious email message as a possibly fraudulent email message.

[c9] A computer system for investigating a suspicious uniform resource locator to determine whether a server referenced by the uniform resource locator may be involved in fraudulent activity, the computer system comprising: a processor; and a computer readable medium in communication with the processor, the computer readable medium comprising instructions executable by the processor to:

ascertain an address associated with a server referenced by the uniform resource locator;

obtain information about an address the uniform resource locator appears to reference;
compare the ascertained address associated with the information about the address the uniform resource locator appears to reference; and
based on the comparison of the ascertained address and the information about the address the uniform resource locator appears to reference, determine whether the uniform resource locator is fraudulent.

[c10] A computer system for investigating a suspicious uniform resource locator as recited in claim 9, wherein computer readable medium comprises further instructions executable to interrogate the server referenced by the uniform resource locator.

[c11] A computer system for investigating a suspicious uniform resource locator as recited in claim 9, wherein computer readable medium comprises further instructions executable to generate an event report.

[c12] A computer system for investigating a suspicious uniform resource locator as recited in claim 10, wherein interrogating the server referenced by the uniform resource locator comprises:
downloading at least one web page from the server referenced by the uniform resource locator; and

analyzing the at least one web page to determine whether the at least one web page comprises a field for allowing a user to provide personal information to the server referenced by the at least one uniform resource locator.

[c13] A computer system for investigating a suspicious uniform resource locator as recited in claim 10, wherein interrogating the server referenced by the uniform resource locator comprises:

examining the server for vulnerabilities that indicate the server possibly has been compromised.

[c14] A computer system for investigating a suspicious uniform resource locator as recited in claim 9, wherein ascertaining an address associated with the server referenced by the uniform locator comprises tracing a route to the server referenced by the uniform resource locator.

[c15] A computer system for investigating a suspicious uniform resource locator as recited in claim 9, wherein obtaining information about an address the uniform resource locator appears to reference comprises parsing an anchor associated with the uniform resource locator to identify an apparent address for a server referenced by the uniform resource locator.

[c16] A computer system for investigating a suspicious uniform resource locator as recited in claim 15, wherein obtaining information about an address the uniform resource locator appears to reference further comprises obtaining WHOIS information about the apparent address for the server referenced by the uniform resource locator.

[c17] A computer system for investigating a suspicious uniform resource locator as recited in claim 9, wherein obtaining information about an address the uniform resource locator appears to reference comprises parsing an anchor associated with the uniform resource locator to identify a trusted entity apparently referenced by the uniform resource locator.

[c18] A computer system for responding to a fraudulent attempt to collect personal information, the computer system comprising:
a processor; and
a computer readable medium in communication with the processor, the computer readable medium comprising instructions executable by the processor to:
download a web page from a suspicious server;
parse the web page to identify at least one field into which a user may enter personal information;
analyze the at least one field to identify a type of in-

formation requested by the at least one field;
generate a set of safe data comprising personal information associated with a fictitious entity;
based on an analysis of the at least one field, select at least a portion of the set of safe data comprising the type of information requested by the at least one field;
format a response to the web page, the response including the portion of the safe data comprising the type of information requested by the at least one field; and
transmit the response to the web page for reception by the suspicious server.

- [c19] A computer system for responding to a fraudulent attempt to collect personal information as recited in claim 18, wherein analyzing the at least one field to identify a type of information requested by the field comprises interpreting a label associated with the at least one field.
- [c20] A computer system for responding to a fraudulent attempt to collect personal information as recited in claim 18, wherein the set of safe data is associated with a financial account, and wherein the computer readable medium comprises further instructions executable by the processor to:
monitor the financial account for an account activity evi-

dencing a use of information obtained from the set of safe data; and
trace the account activity to identify an entity using the information obtained from the set of safe data.

[c21] A computer system for responding to a fraudulent attempt to collect personal information as recited in claim 18, wherein the computer readable medium comprises further instructions executable by the processor to:
generate a plurality of sets of safe data, each of the sets of safe data comprising personal information associated with a fictitious entity;
based on an analysis of the at least one field, select at least a portion of each of the sets of safe data responsive to the at least one field;
format a plurality of responses to the web page, each of the plurality of response including the portion of one of the sets of safe data, each of the portions of one of the sets of safe data being responsive to the at least one field; and
transmit the plurality of responses to the web page for reception by the suspicious server.

[c22] A computer system for responding to a fraudulent attempt to collect personal information as recited in claim 21, wherein the computer readable medium comprises further instructions executable by the processor to:

transmit for reception by the suspicious server a number of responses to the web page sufficient to cause a recipient of the responses to be uncertain which of a plurality of responses include valid personal information.

[c23] A computer system for responding to a fraudulent attempt to collect personal information as recited in claim 21, wherein the computer readable medium comprises further instructions executable by the processor to: transmit for reception by the suspicious server a number of responses to the web page sufficient to indicate that the fraudulent attempt to collect personal information has been discovered.

[c24] A computer system for responding to a fraudulent attempt to collect personal information as recited in claim 21, wherein the computer readable medium comprises further instructions executable by the processor to: transmit for reception by the suspicious server a number of responses to the web page sufficient to prevent the suspicious server from receiving any responses comprising valid personal information.

[c25] In a relationship between a fraud protection provider and a customer, a system for combating online fraud, the system comprising:
a monitoring center for monitoring a suspicious email

activity, the monitoring center comprising a first computer, the first computer including instructions executable by the first computer to allow the analysis of the suspicious email activity and the initiation of a response to the suspicious email activity;

a second computer in communication with the monitoring center, the second computer including instructions executable by the second computer to:

- gather an incoming email message addressed to at least one bait email address that has been seeded at a location on a computer network likely to be a target for a third party attempting to harvest email addresses, the incoming email message including a uniform resource locator configured to direct a recipient of the incoming email message to a web site referenced by the uniform resource locator; and

a third computer in communication with the second computer and further in communication with the monitoring center, the third computer including instructions executable by the third computer to:

- analyze the incoming email message;
- based on an analysis of the incoming email message, categorize the incoming email message as a fraudulent email message;
- investigate the uniform resource locator included with the incoming email message to determine infor-

mation about a server hosting the web site referenced by the uniform resource locator; and
prepare a report comprising at least some of the information about the server hosting the web site referenced by the uniform resource locator.

- [c26] A system for combating online fraud as recited in claim 25, wherein the first computer includes further instructions executable by the first computer to notify the customer that a fraudulent email message has been received.
- [c27] A system for combating online fraud as recited in claim 25, wherein the first computer includes further instructions executable by the first computer to analyze the suspicious email activity.
- [c28] A system for combating online fraud as recited in claim 25, wherein the first computer includes further instructions executable by the first computer to allow a technician to analyze the suspicious email activity.
- [c29] A system for combating online fraud as recited in claim 25, wherein the first computer and the second computer are the same computer.
- [c30] A system for combating online fraud as recited in claim 25, wherein the second computer and the third computer

are the same computer.

- [c31] A system for combating online fraud as recited in claim 25, wherein the first computer includes further instructions executable by the first computer to allow a technician to initiate an administrative response against an operator of the server.
- [c32] A system for combating online fraud as recited in claim 25, wherein the first computer includes further instructions executable by the first computer to pursue an administrative response against an operator of the server.
- [c33] A system for combating online fraud as recited in claim 25, wherein the first computer includes further instructions executable by the first computer to allow a technician to initiate a technical response against an operator of the server hosting the web site referenced by the uniform resource locator.
- [c34] A system for combating online fraud as recited in claim 33, the system further comprising a set of at least one computer, each computer of the set of at least one computer including instructions executable by that computer to pursue a technical response against the server.
- [c35] A system for combating online fraud as recited in claim 34, wherein the set of at least one computer comprises a

plurality of computers, such that pursuing a technical response against the server comprises pursuing a distributed technical response against the server.

- [c36] A computer software application that is executable by a computer to:
- create at least one safe account, the at least one safe account being associated with at least one bait email address;
 - seed the at least one bait email address at a location on a computer network, the location being a likely target for a third party attempting to harvest email addresses;
 - gather an incoming email message addressed to the at least one bait email address, the incoming email message including a uniform resource locator configured to direct a recipient of the incoming email message to a web site referenced by the uniform resource locator;
 - analyze the incoming email message;
 - based on an analysis of the incoming email message, categorize the incoming email message as a possibly fraudulent email message;
 - investigate the uniform resource locator included with the incoming email message to determine information about a server hosting the web site referenced by the uniform resource locator;
 - prepare a report comprising at least some of the infor-

mation about the server hosting the web site referenced by the uniform resource locator; and
allow an analysis of the report to determine whether the server is likely to attempt to fraudulently collect personal information.

[c37] A computer software application as recited in claim 36, wherein the computer software application is further executable by a computer to analyze the report to determine whether the server is likely to attempt to fraudulently collect personal information.

[c38] A computer software application as recited in claim 36, wherein the computer software application is further executable by a computer to allow a technician to initiate an action in response to a fraudulent attempt by the server to collect personal information.

[c39] A computer software application as recited in claim 36, wherein the computer software application is further executable by a computer to pursue an action in response to a fraudulent attempt by the server to collect personal information.

[c40] A computer software application as recited in claim 36, wherein the computer software application comprises a plurality of interoperable software modules, such that

each of the plurality of interoperable software modules is executable by a different computer.

[c41] A computer readable medium embodying the computer software application of claim 36.

[c42] A computer system configured to execute the computer software application of claim 36.

[c43] In a relationship between a fraud protection provider and a customer, a method of combating online fraud, the method comprising:

creating at least one safe account, the at least one safe account being associated with at least one bait email address;

seeding the at least one bait email address at a location on a computer network, the location being a likely target for a third party attempting to harvest email addresses;

gathering an incoming email message addressed to the at least one bait email address, the incoming email message including a uniform resource locator configured to

direct a recipient of the incoming email message to a web site referenced by the uniform resource locator;

analyzing the incoming email message;

based on an analysis of the incoming email message, categorizing the incoming email message as a fraudulent email message;

investigating the uniform resource locator included with the incoming email message to determine information about a server hosting the web site referenced by the uniform resource locator;

preparing a report comprising at least some of the information about the server hosting the web site referenced by the uniform resource locator;

analyzing the report to determine whether the server is engaged in a fraudulent attempt to collect personal information; and

taking an action to respond to the fraudulent attempt to collect personal information.

[c44] A method of combating online fraud as recited in claim 43, wherein the bait email address is seeded at a location selected from the group consisting of a domain registration record, a newsgroup, an electronic mailing list, an electronic customer list, an online chat room, an online message board and a list of active email addresses.

[c45] A method of combating online fraud as recited in claim 43, wherein the incoming email message purports to be from the customer.

[c46] A method of combating online fraud as recited in claim 45, wherein the method further comprises establishing a customer profile for the customer, wherein the customer

profile includes instructions governing how an attempted online fraud should be handled, and wherein taking an action to respond to the fraudulent collection of personal information comprises consulting the customer profile to determine which of a plurality of actions to take to respond to the fraudulent collection of personal information by the server.

[c47] A method of combating online fraud as recited in claim 45, wherein taking an action to respond to the fraudulent collection of personal information by the server comprises notifying the customer of the fraudulent attempt to collect personal information.

[c48] A method of combating online fraud as recited in claim 43, wherein taking an action to respond to a fraudulent attempt by the server to collect personal information comprises pursuing an administrative response against an operator of the server.

[c49] A method of combating online fraud as recited in claim 48, wherein pursuing an administrative response against an operator of the server comprises notifying an Internet service provider associated with the server that the server is engaged in a fraudulent activity.

[c50] A method of combating online fraud as recited in claim

43, wherein the information about the server indicates that the server has been used compromised in a fraudulent attempt to collect personal information, and wherein taking an action to respond to a fraudulent attempt by the server to collect personal information comprises notifying an operator of the server that the server has been compromised.

[c51] A method of combating online fraud as recited in claim 43, wherein investigating the uniform resource locator included with the incoming email message to determine information about a server hosting the web site referenced by the uniform resource locator comprises identifying at least one field for providing personal information to a web page hosted by the server.

[c52] A method of combating online fraud as recited in claim 51, wherein investigating the uniform resource locator included with the incoming email message to determine information about a server hosting the web site referenced by the uniform resource locator comprises downloading at least one web page from the server, and wherein the at least one web page requests personal information.

[c53] A method of combating online fraud as recited in claim 51, wherein taking an action to respond to a fraudulent

attempt by the server to collect personal information comprises pursuing a technical response against the server.

[c54] A method of combating online fraud as recited in claim 53, wherein pursuing a technical response against the server comprises providing fictitious personal information to the server, and wherein the fictitious personal information is formatted to be responsive to the at least one field for providing personal information to a web page hosted by the server.

[c55] A method of combating online fraud as recited in claim 54, wherein the fictitious personal information provided to the server comprises a traceable identifier, and wherein pursuing a technical response against the server comprises tracing a use of the traceable identifier.

[c56] A method of combating online fraud as recited in claim 55, wherein the traceable identifier comprises an account identifier for a financial account associated with the customer.

[c57] A method of combating online fraud as recited in claim 54, wherein pursuing a technical response against the server comprises providing sufficient fictitious personal information to impede the use of any valid personal in-

formation received by the server.

- [c58] A method of combating online fraud as recited in claim 54, wherein pursuing a technical response against the server comprises providing sufficient fictitious personal information to notify an operator of the server that the attempt to fraudulently collect personal information has been discovered.
- [c59] A method of combating online fraud as recited in claim 54, wherein pursuing a technical response against the server comprises providing fictitious personal information at a rate sufficient to impede the server's ability to receive personal information from any other sources.
- [c60] A method of combating online fraud as recited in claim 54, wherein pursuing a technical response against the server comprises transmitting the fictitious personal information from a plurality of computers.
- [c61] A method of combating online fraud as recited in claim 43, wherein investigating the uniform resource locator included with the incoming email message to determine information about a server hosting the web site referenced by the uniform resource locator comprises accessing a set of WHOIS information about an apparent address referenced by the uniform resource locator.

- [c62] A method of combating online fraud as recited in claim 43, wherein investigating the uniform resource locator included with the incoming email message to determine information about a server hosting the web site referenced by the uniform resource locator comprises ascertaining an Internet Protocol address referenced by the uniform resource locator.
- [c63] A method of combating online fraud as recited in claim 43, wherein investigating the uniform resource locator included with the incoming email message to determine information about a server hosting the web site referenced by the uniform resource locator comprises interrogating the server hosting the web site referenced by the uniform resource locator.
- [c64] A method of combating online fraud as recited in claim 43, wherein investigating the uniform resource locator included with the incoming email message to determine information about a server hosting the web site referenced by the uniform resource locator comprises tracing a network route to the server.
- [c65] A method of combating online fraud as recited in claim 43, wherein analyzing the incoming email message comprises analyzing a header portion of the incoming email

message.

- [c66] A method of combating online fraud as recited in claim 65, wherein analyzing a header portion of the incoming email message comprises determining whether the incoming message is a spoofed message.
- [c67] A method of combating online fraud as recited in claim 65, wherein analyzing a header portion of the incoming email message comprises determining whether the incoming email message originates from a suspicious Internet domain.
- [c68] A method of combating online fraud as recited in claim 43, wherein analyzing the incoming email message comprises analyzing a body portion of the incoming email message.
- [c69] A method of combating online fraud as recited in claim 68, wherein analyzing a body portion of the incoming message comprises searching the body portion of the incoming message for strings indicating that the incoming message may be part of an attempt to fraudulently collect personal information.
- [c70] A method of combating online fraud as recited in claim 43, wherein analyzing the incoming email message comprises analyzing a uniform resource locator included in

the incoming email message.

- [c71] A method of combating online fraud as recited in claim 70, wherein analyzing a uniform resource locator included in the incoming email message comprises determining whether the uniform resource locator references a suspicious Internet location.
- [c72] A method of combating online fraud as recited in claim 43, wherein analyzing the incoming email message comprises assigning a score to the incoming email message.
- [c73] A method of combating online fraud as recited in claim 72, wherein analyzing the incoming email message further comprises comparing the assigned score with a threshold score.